UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	C.A. 12-MD-2358 (SLR)
This Document Relates to: **All Actions**	

DEFENDANT GOOGLE INC.'S
REPLY BRIEF IN SUPPORT OF ITS
MOTION TO DISMISS THE CONSOLIDATED AMENDED COMPLAINT

COLLEEN BAL, CA Bar No. 167637
MICHAEL H. RUBIN, CA Bar No. 214636
ANTHONY J WEIBELL, CA Bar No. 238850
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
650 Page Mill Road
Palo Alto, CA 94304-1050
Telephone: (650) 493-9300
Facsimile: (650) 565-5100
E-mail: cbal@wsgr.com; mrubin@wsgr.com;
aweibell@wsgr.com

Attorneys for Defendant
GOOGLE INC.

April 26, 2013

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

I. INTRODUCTION

Plaintiffs contend in their Opposition to Google's Motion to Dismiss that Google has unfairly "portrayed" the facts they set out in their Consolidated Amended Complaint ("CAC"). *See, e.g.*, Opp. at 1, 5. But Google's Motion is based only on allegations taken directly from the CAC and from documents that the CAC incorporated by reference (which are the subject of Google's *unopposed* Request for Judicial Notice ("RJN")). While Google disregarded Plaintiffs' rhetoric and conclusory assertions, that is precisely what is required on this motion.[1]

The facts pleaded by Plaintiffs confirm that they suffered no injury and cannot state a claim. Although Plaintiffs allege that Google placed unwanted cookies on their browsers and thereby obtained information from them, Plaintiffs' own allegations reveal that their browsers would have sent the same Browser-Generated Information ("BGI") to Google—including what they claim was "personal information" or "PII"—whether or not Google had ever placed cookies on their browsers. *See* CAC ¶¶ 30-33, 41, 84-96, 205; Mot. at 3-4. Those allegations require dismissal of Plaintiffs' CAC. According to Plaintiffs: when a website URL is entered into a browser's address bar, the browser submits a "GET" request to the website seeking all content displayed on the website. *Id.* ¶¶ 31, 85. The browser's GET request includes certain information about the browser, including its IP address, the URL of the website the browser wants to view, the browser's screen resolution, and other BGI, so that the website can provide the correct response. *Id.* ¶¶ 33, 46. If the website wishes to display a Google ad, the website will respond with an instruction to the browser to send a separate GET request to Google to obtain ad content. *Id.* ¶¶ 41, 86. In response, the browser sends a separate GET request to

[1] *See Pearson v. Tanner*, No. 12-2503, 2013 WL 432377, at *1 (3d Cir. Feb. 5, 2013) ("legal conclusions" and "bald assertions" must be disregarded) (quoting *Morse v. Lower Merion Sch. Dist.*, 132 F.3d 902, 906 (3d Cir. 1997)). Rhetoric used to color facts is also disregarded, as courts will decide a motion to dismiss "not upon the presence of mere words" in the complaint, "but, rather, upon the presence of a factual situation which is or is not justiciable," and will draw on the complaint's allegations "in a realistic, rather than a slavish, manner." *Id.* (quoting *Doug Grant, Inc. v. Greate Bay Casino Corp.*, 232 F.3d 173, 184 (3d Cir. 2000).

Google, complete with the BGI necessary to respond with the correct display instructions, including the URL information that Plaintiffs allege contains their PII. *Id.* ¶¶ 41, 47, 87, 205.

No cookie plays a role in the communication of BGI to Google, and Plaintiffs do not allege otherwise. Indeed, Plaintiffs' allegations about the two Google cookies at issue—the DoubleClick ID Cookie and the Intermediary Cookie—serve only to drive this point home:

- *The DoubleClick ID Cookie.* If a DoubleClick ID Cookie is present on a browser that visits a webpage wishing to display a Google ad, the value of that cookie is sent to Google as part of the GET request for that ad. Plaintiffs do not allege that the cookie value itself contains any BGI or that they have any proprietary interest in the cookie value. Rather, the CAC concedes that the cookie value is just a string of characters that allows Google to "associate" multiple instances of BGI received from the same browser. *Id.* ¶¶ 46, 78, 205. Thus, while Plaintiffs argue that Google used DoubleClick ID Cookies to "collect" information (Opp. at 4), that argument is refuted by the controlling CAC allegations. CAC ¶¶ 41, 46; *see also* Opp. at 18 (conceding that the DoubleClick ID cookie merely "allow[s] Google to associate" BGI already sent to Google with a unique cookie value). These allegations make clear that the DoubleClick ID Cookie did not cause Google to receive Plaintiffs' BGI. Google would have received that information with or without the cookie.

- *The Intermediary Cookie.* Plaintiffs argue in their Opposition that Google "collects" "user information" (or "account information" or "user-specific information") and "combines" or "links" it with BGI using the Intermediary Cookie. *See* Opp. at 4-5. But the CAC confirms that this is a red herring. To the extent the Intermediary Cookie "links" any user account information with BGI, it does so only where a user (1) has signed up for a Google Account, (2) has *consented* to the linking under Google's Terms of Service and Privacy Policy, and (3) is signed-in to a Google Account at the time a Google ad is encountered. *See* CAC ¶ 98 n.66 (citing privacy policy); RJN Ex. 1 at 1-3; RJN Ex. 3 at 4; *see also* Mot. at 5, 9 & n.7. In *all* other instances, the CAC concedes that the Intermediary Cookie is "blank." CAC ¶ 78; RJN Ex. 3 at 4. Plaintiffs do not claim to be Google account

holders, much less account holders who satisfied these three conditions under which the Intermediary Cookie would have made any difference. *See* CAC ¶¶ 10-13. If Plaintiffs received an Intermediary Cookie, it would have been a "blank" version, not one capable of "linking" their Google Account information with BGI. *Id.* ¶ 78. And regardless, the Intermediary Cookie plays no role in transmitting BGI to Google.

These allegations show the fundamental disconnect in Plaintiffs' case: there is no connection between the conduct at issue (Google's alleged placement of cookies) and the harm Plaintiffs claim resulted from that conduct (Google's receipt of Plaintiffs' BGI). Because the conduct Plaintiffs allege did not cause them any harm, they lack standing. Beyond that gating issue, they also fail to state a single claim. Accordingly, the CAC should be dismissed in its entirety.

II. PLAINTIFFS CANNOT SHOW THEY HAVE ARTICLE III STANDING

A. Plaintiffs Cannot Identify Any Injury-In-Fact

Plaintiffs cannot show any injury to establish Article III standing, not even a "trifle." *See* Opp. at 8. That is no surprise: (1) the placement or presence of cookies on Plaintiffs' browsers did not cause Google to receive any BGI, and (2) even if one assumed (incorrectly) that Google received BGI from or because of the cookies, Plaintiffs' vague and unsupported allegations of diminution in the value of their PII is not a cognizable injury. Mot. at 12-15.

In opposition, Plaintiffs point to their allegations that "studies" show "PII has identifiable value to Plaintiffs" and that "Google itself pays users for PII" to try to show injury. Opp. at 11, 13 (citing CAC ¶¶ 56-67). These allegations do not help Plaintiffs. *First*, courts uniformly reject claims of injury—and thus Article III standing—based on generalized allegations that the value of a plaintiff's "PII" has been diminished by its unauthorized collection or use. *See* Mot. at 13-15 (citing cases); *Yunker v. Pandora Media, Inc.*, No. 11-3113, 2013 WL 1282980, at *4 (N.D. Cal. Mar. 26, 2013). Plaintiffs allege no more than the abstract claims of injury consistently rejected in prior decisions. In fact, Plaintiffs allege even *less*: prior decisions have involved allegations of actual collection and use of PII, whereas Plaintiffs' allegations show that no PII was collected or used based on the conduct they challenge. *Supra* pp. 1-3.

Second, the allegations and "studies" cited by Plaintiffs have no connection to Plaintiffs or to this case. None of their allegations or cited studies involves a consumer receiving payment for the type of information sent by Plaintiffs' browsers to Google when they visited websites displaying Google ads. *Compare* CAC ¶ 56 (study estimating amount users would *pay* (not receive) to keep private their complete, non-anonymous "browsing histories"), ¶¶ 57-60 (Google Screenwise program set up to pay panelists to provide their complete, non-anonymous BGI and browser history in connection with test of Google Chrome browser), ¶¶ 61-67 (news reports about businesses that sell services based on protection or use of unspecified PII).

Nor do Plaintiffs show that any named plaintiff has "personally been harmed," an undisputed requirement. Opp. at 9. Plaintiffs argue that the CAC shows "Google invaded Plaintiffs' computers and took their information," *id*. at 10 (citing CAC ¶¶ 1-5, 10-13, 68-126), but the 67 cited paragraphs show nothing like that. In fact, the *only* allegations specific to the named plaintiffs are that they used a Safari or IE browser in its default state to "review[] and transmit[] confidential and personal information and [to] visit[] websites with third-party advertisements of the Defendants." CAC ¶¶ 10-13. The named plaintiffs allege no specific websites they visited and no specific information that Google allegedly obtained from them. And despite claiming a reduction in the value of their "PII," Plaintiffs allege no attempted but frustrated sale, no reduced offer to purchase, nor even a market where those hypothetical transactions might take place. On top of all that, Plaintiffs do not even allege facts showing that Google placed cookies on their browsers. In sum, Plaintiffs allege no concrete injury whatsoever.

B. Plaintiffs Cannot Establish Standing by Invoking Inapplicable Statutes

Plaintiffs contend that even without actual injury, they have Article III standing because they have asserted statutory claims under the Wiretap Act and Stored Communications Act ("SCA"). Opp. at 10. They are mistaken. While it is by no means clear that plaintiffs who have suffered no injury-in-fact can bring a claim under the Wiretap Act or SCA, it is clear that they must at a minimum state a claim under those statutes to be able to invoke a theory of statutory standing. *See* 18 U.S.C. § 2520(a) (standing under Wiretap Act requires facts showing plaintiff's

electronic communications were "intercepted, disclosed, or intentionally used in violation of [the Wiretap Act]"); 18 U.S.C. § 2707(a) (standing under SCA requires facts showing plaintiff has been "aggrieved by any violation of [the SCA]"); *In re Google Inc. Privacy Policy Litig.*, No. 12-1382, 2012 WL 6738343, at *5-6 (N.D. Cal. Dec. 28, 2012) (deficient Wiretap Act claim cannot confer Article III standing); *Sterk v. Best Buy Stores, L.P.*, No. 11-1894, 2012 WL 5197901, at *5 (N.D. Ill. Oct. 17, 2012) ("plaintiff must plead [both] an injury [and] a statutory violation to meet the standing requirement of Article III [for an SCA claim]").

As detailed in Google's opening brief and below, Plaintiffs have not stated a claim under the Wiretap Act or the SCA. Because they cannot rely on these statutes to confer statutory standing and fail to plead any injury-in-fact, the Court need go no further than its analysis of the Wiretap Act and SCA claims to dismiss the complaint in its entirety for lack of Article III standing.[2]

III. PLAINTIFFS CANNOT STATE A CLAIM

A. Plaintiffs Cannot State a Federal Wiretap Claim

1. Google Was a Party to Plaintiffs' Communications

Google's receipt of BGI from Plaintiffs' browsers did not violate the Wiretap Act because Google was a party to those communications. Plaintiffs' browsers communicated BGI directly to Google in the form of GET requests for ads. CAC ¶¶ 41, 86; *see* Mot. at 16. In opposition, Plaintiffs argue that Google was not an authorized party to those communications because their browsers were "configured to prohibit Google from becoming a party to them" and because Google "tricked" their browsers into sending Google the BGI communicated to the websites displaying Google ads. Opp. at 14. The facts pleaded in the CAC show otherwise. Each time Plaintiffs visited a website displaying a Google ad, Plaintiffs' browsers voluntarily sent to Google the BGI Plaintiffs now contend was unlawfully intercepted, *whether or not Plaintiffs' browsers had any Google cookies*. *Supra* pp. 1-3. Plaintiffs, through their browsers,

[2] It appears Plaintiffs may also contend that they can establish standing merely by asserting claims under other statutes. Opp. at. 11. Not so. Each of the other statutes at issue expressly hinges standing on a showing of injury-in-fact, and Plaintiffs cannot make that showing. *See infra* pp. 10-11 (CFAA), 13 (CCL), 15-16 (CLRA), 16 (UCL); *see also* Cal. Pen. Code § 637.2.

communicated directly with Google, not through any "trick," and not by virtue of any cookie, but because that is how browsers obtain advertising content. *See* CAC ¶ 41. To the extent any communications took place, Google was an authorized party to them.

2. The "Prior Consent" Exception Precludes the Wiretap Claim

Even under Plaintiffs' factually-incorrect theory that their browsers only communicated with websites that displayed Google ads (and not also and separately with Google), their wiretap claim should be dismissed because Google had "prior consent" from those websites to receive the communications. CAC ¶ 41; Mot. at 17 (citing 18 U.S.C. § 2511(2)(d)). Plaintiffs argue that the "prior consent" exception is an affirmative defense that cannot be raised on a motion to dismiss, and that Google must provide "evidence" that "all" websites visited by Plaintiffs "consented to its conduct." Opp. at 15-16. They are incorrect. Even if "prior consent" were an affirmative defense, a complaint may be dismissed where the affirmative defense "appears on its face." *Victaulic Co. v. Tieman*, 499 F.3d 227, 234-35 (3d Cir. 2007); *see also In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 510, 514 (S.D.N.Y. 2001) (dismissing wiretap claim because consent was apparent from allegations in complaint). Here, as in *DoubleClick*, consent is apparent from the face of the CAC because the websites on which the Google ads appeared necessarily enabled and thereby authorized Google to receive GET requests and return ads. *See, e.g.*, CAC ¶ 41 (describing process by which "host" websites instruct browsers to send GET requests directly to Google).

Plaintiffs' effort to distinguish *DoubleClick* on the ground that it did not involve allegations of "intentional circumvention of privacy settings" (Opp. at 16) misses the point.[3] Regard-

[3] Plaintiffs argue incorrectly that their browsers were set "to block any cookies from being deposited." *See, e.g.*, Opp. at 13. As the CAC itself explains, the default settings of Plaintiffs' browsers did not block "any cookies" from being placed—the default settings actually permitted third party cookies to be placed in a number of circumstances. *See* Mot. at 6-9; RJN Ex. 3. Similarly, Plaintiffs claim throughout their opposition brief to have set a "do not track" feature on their browsers. *See, e.g.*, Opp. at 13. That is not supported by the prevailing allegations of the CAC, which show that Plaintiffs used their browsers' default settings for third party cookie handling, not that Plaintiffs employed a separate "do not track" feature. The two are not the same. *See* http://donottrack.us; http://www.ftc.gov/opa/reporter/privacy/donottrack.shtml.

less of "privacy settings" and whether or not any cookies were present on users' browsers, the websites on which Google ads appeared instructed Plaintiffs' browsers to send GET requests to Google, thereby communicating Plaintiffs' BGI to Google. Plaintiffs' allegations about the placement and presence of cookies are irrelevant to the analysis, as are Plaintiffs' allegations that a few websites now claim they were unaware of how Google placed cookies. Opp. at 15-16. If Google received Plaintiffs' BGI, it did so only because a website on which Google ads appeared instructed Plaintiffs' browsers to send that information to Google as a GET request.[4]

3. Google Did Not Unlawfully Intercept Any "Contents"

Plaintiffs admit that they must show Google intercepted the "contents" of their communications to state a wiretap claim, yet they do not dispute that the cookies themselves are not the "contents" of a communication. *See* Mot. at 17-19; Opp. at 16; 18 U.S.C. §§ 2510(4, 8), 2511(1). Nor do Plaintiffs dispute that the only potential "contents" that Google received were BGI. *See* Opp. at 17. To the extent the Wiretap Act covers any BGI, Google's receipt of BGI would not be actionable because Plaintiffs' browsers voluntarily sent it directly to Google regardless of the presence of any cookies. CAC ¶¶ 86-87; *supra* pp. 1-3, 5-6. Thus, no unlawful interception occurred, and Plaintiffs' Wiretap Act claim fails. *See* 18 U.S.C. § 2511(2)(d).

While Plaintiffs argue that Google placed cookies that "allow[ed]" Google "to associate vast amounts of communications content" that Plaintiffs' browsers sent to Google when visiting websites displaying Google ads, Opp. at 18, that is an argument concerning Google's *use* of communications, not an argument that Google *intercepted* them. Because the Wiretap Act only prohibits use of communications that are unlawfully intercepted (18 U.S.C. § 2511(2)(d)), and because the BGI was not unlawfully intercepted—it was voluntarily sent to Google—any "association" of Plaintiffs' BGI could not violate the Wiretap Act. *See* Mot. at 19. Indeed, Plain-

[4] Plaintiffs' contention that Google is prevented from relying on the prior consent exception because Plaintiffs have asserted a claim for invasion of privacy is misplaced. *Id*. at 15 n.6. Although consent can be negated if the communication is intercepted for the purpose of committing a "criminal or tortious act," 18 U.S.C. § 2511(2)(d), the intent of the interception must actually be to commit a tort or crime that is separate from the interception itself. *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010). No such intent is or could be alleged here.

tiffs concede that their "use and disclosure" claims rise or fall with their interception claim. *See* Opp. at 18. Because there was no unlawful interception, the Wiretap Act was not violated.[5]

B. Plaintiffs Cannot State a Stored Communications Act Claim

1. Plaintiffs Fail to Identify a Communication "in Electronic Storage"

Plaintiffs' Wiretap Act and SCA claims are irreconcilable. The wiretap claims allege that Google obtained communications "in transit" and accessed them "contemporaneously with the[ir] transmission." CAC ¶¶ 208, 266. Those allegations preclude the SCA claim—which requires communications to be accessed while in "electronic storage"—since communications "in transit" cannot simultaneously be "in storage." 18 U.S.C. § 2701(a); *United States v. Smith*, 155 F.3d 1051, 1058 (9th Cir. 1998). Plaintiffs' inability to plead facts supporting the required "electronic storage" element alone requires dismissal of their SCA claim. *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1059 (N.D. Cal. 2012) ("*iPhone II*").

Plaintiffs' SCA claim fails for another reason: the SCA does not apply to information on a consumer's personal device. Since Plaintiffs do not dispute that the SCA only applies to communications stored by an "electronic communication service provider" ("ECS provider") in a "facility" through which the ECS is provided, they contort the statute to try to make the elements fit their facts. *See* Opp. at 20; CAC ¶ 217; Mot. at 20-21. Plaintiffs' brand new theory (not alleged in the CAC) is that Google is "an [ECS] provider" with respect to the placement of the DoubleClick ID Cookie on their browsers; Plaintiffs' "browser-managed files" are part of Google's "facilities"; and the cookies are stored "temporarily" on Plaintiffs' personal devices by Google. *See* Opp. at 20-22 & nn. 9-10. This new theory fails for three reasons.

[5] Plaintiffs' California wiretap claim (Count VIII) should likewise be dismissed because Plaintiffs' browsers voluntarily communicated BGI directly to Google, and Google therefore did not intercept any communications. CAC ¶¶ 41, 86-87; *Powell v. Union Pac. R.R. Co.*, 864 F. Supp. 2d 949, 955 (E.D. Cal. 2012); *Membrila v. Receivables Performance Mgmt., LLC*, No. 09-2790, 2010 WL 1407274, at *2 (S.D. Cal. Apr. 6, 2010). Plaintiffs' argument that Google "willfully" intercepted Plaintiffs' communications because of how it placed cookies on their browsers (Opp. at 32-33) once again ignores that Google would have received BGI from Plaintiffs' browsers whether or not any cookie were present. *Supra* pp. 1-3. To the extent communications occurred between Plaintiffs' browsers and websites showing Google ads, Google never received those communications, by interception or otherwise. CAC ¶¶ 41, 86-87.

First, Plaintiffs' new theory contradicts the CAC. The CAC alleges that (i) Plaintiffs' Safari and IE browsers (not Google) are the ECS providers; (ii) the cookies are "persistent" (not temporary) and "could stay on a user's device for years"; (iii) the cookies are stored by Plaintiffs' browsers (not by Google); and (iv) the cookies are stored on Plaintiffs' devices (not in a Google facility). *See* CAC ¶¶ 39(a)(ii), 216-218. Because they diverge from the CAC, the new "allegations" in Plaintiffs' Opposition must be ignored.

Second, even if Plaintiffs' new theory could be considered, Plaintiffs' claim that Google was acting as an ECS provider here (Opp. at 20 n.10) is not defensible. Google was not acting as an Internet service or email provider, nor otherwise providing Plaintiffs with "the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (defining ECS); *see DoubleClick*, 154 F. Supp. 2d at 509. That an entity may offer email services in one part of its business does not render it an ECS provider as to unrelated aspects of its business.[6] *See Shefts v. Petrakis*, No. 10-1104, 2013 WL 489610, at *5 (C.D. Ill. Feb. 8, 2013).

Third, courts have overwhelmingly rejected Plaintiffs' theory that their personal computers and devices (and by extension the "browser-managed files" and cookies on them) are "facilities" under the SCA. They have done so because that interpretation would pervert the statute's goals. *See, e.g., iPhone II*, 844 F. Supp. 2d at 1058 (rejecting argument that user's computer is a "facility" under the SCA since "adopting [that] construction would render other parts of the statute illogical"); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270-71 (N.D. Cal. 2001) (rejecting plaintiff's argument that a user's computer is a "facility" under the SCA, since in light of other provision of SCA authorizing access to a "facility" by an ECS provider, plaintiff's interpretation would allow ECS providers to grant third parties access to users' home computers). These courts recognize that the SCA covers only physical "'facilities that

[6] If Plaintiffs were correct that Google was acting as an ECS provider here, Google would have been *authorized* under the terms of the statute to access the files it allegedly stored on Plaintiffs' devices, and Plaintiffs' SCA (as well as their Wiretap Act) claims would still fail. 18 U.S.C. § 2701(c)(1) (ECS provider authorized to access stored communications); *Yunker*, 2013 WL 1282980, at *9; *see also* 18 U.S.C. § 2510(5); *Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1250-51 (10th Cir. 2012).

are *operated by*'" ECS providers, such as the providers' servers, not users' devices. *Shefts*, 2013 WL 489610, at *4 (quoting *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 792 (5th Cir. 2012)); *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 334-35 (D.D.C. 2011) (no SCA claim if access was only to plaintiffs' computers; access must be to servers or networks); *see also* D.I. 62 at 15.[7]

2. Plaintiffs Cannot Allege Unauthorized Access

The SCA claim also fails because Plaintiffs cannot plead unauthorized access to a stored communication. Although the CAC is vague about what stored information Google allegedly accessed—BGI or cookie values—the CAC is clear that Plaintiffs' browsers *sent* that information to Google voluntarily. CAC ¶¶ 41, 218; *supra* pp. 1-3. Either way, there was no unauthorized access. Plaintiffs' assertion that the "illicit placement" of cookies constitutes unauthorized access is wrong. Placing a cookie is not accessing a communication "in electronic storage" and is thus not covered by the statute. *See* 18 U.S.C. § 2701(a).

C. Plaintiffs Cannot State a Federal Computer Fraud and Abuse Act Claim

1. Plaintiffs Have Not Alleged "Damage" or "Loss"

Plaintiffs admit that they are required to show "damage" or "loss" to have standing under the Computer Fraud and Abuse Act ("CFAA"). *See* 18 U.S.C. § 1030(g). But the only "loss" alleged by Plaintiffs (the alleged diminution in value of their PII) is unsupported by the CAC and not cognizable under the law, and the CAC makes no allegation of any "damage." Mot. at 23; *supra* pp. 3-4. In opposition, Plaintiffs manufacture an implausible damage allegation that appears nowhere in the CAC: that Google "impair[ed] the integrity" of their "browser

[7] To support their contention that their personal computers are "facilities," Plaintiffs cite outlier cases that have been rejected by subsequent courts because they "provide little analysis on this point of law, instead assuming plaintiff's position to be true due to lack of argument and then ultimately ruling on other grounds." *iPhone II*, 844 F. Supp. 2d at 1057-58 (disagreeing with *Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001)); *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1275 n.3 (C.D. Cal. 2001); *Expert Janitorial, LLC v. Williams*, No. 09-283, 2010 WL 908740, at *5 (E.D. Tenn. Mar. 12, 2010) (citing *In re Intuit*)). Similarly, the unpublished slip opinion, *Cousineau v. Microsoft Corp.*, No. 11-1438, at 10-11 (W.D. Wash. June 22, 2012), cited by Plaintiffs determined that a mobile phone could be a facility without even considering the weight of authority holding otherwise.

'system'" and "data" by placing "illicit cookies" and "captur[ing their data]." Opp. at 24. Plaintiffs cannot amend their complaint with new "allegations" in their opposition. *Pa. ex rel. Zimmerman v. PepsiCo, Inc.*, 836 F.2d 173, 181 (3d Cir. 1988). But even if they could, courts have repeatedly recognized that cookies do not "impair" computing devices, and Plaintiffs do not identify any impairment they allegedly suffered. *See, e.g.*, *Del Vecchio v. Amazon.com, Inc.*, No. 11-366, 2012 WL 1997697, at *5 (W.D. Wash. Jun. 1, 2012); *LaCourt v. Specific Media, Inc.*, No. 10-1256, 2011 WL 1661532, at *6 (C.D. Cal. Apr. 28, 2011). Because Plaintiffs allege no damage or loss, the Court need go no further to dismiss the CFAA claim.

Even if Plaintiffs could allege a cognizable loss, they fail to show $5,000 in economic loss, a requirement for CFAA standing. 18 U.S.C. §§ 1030(c)(4)(A)(i)(I), 1030(g); *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005). Curiously, Plaintiffs argue that they are *not* required to show a $5,000 economic loss. Opp. at 25. That is wrong. The express language of the CFAA's standing provision (§ 1030(g)) requires Plaintiffs to allege at least one of the injuries listed in Section 1030(c)(4)(A)(i)(I)-(V), and the *only* listed injury that could possibly apply here is in subpart I: a "loss" of "at least $5,000." *See* Mot. at 23-24. Plaintiffs' reliance on *Oracle* is misplaced because *Oracle* only analyzed whether the plaintiff had to show $5,000 in damage to prove a violation under Section 1030(a)(4); the *Oracle* court did not analyze whether a $5,000 economic loss was also required for standing under Section 1030(g). *See Oracle Am., Inc. v. Serv. Key, LLC*, No. 12-790, 2012 WL 6019580, at *3, *4 (N.D. Cal. Dec. 3, 2012).

Plaintiffs also argue that they can aggregate loss across the putative class to try to reach the $5,000 threshold. *See* Mot. at 24 n.12. But aggregation across multiple devices is improper in a private class action; "only federal prosecutors may aggregate losses across multiple protected computers from a related course of conduct." *Lyons v. Coxcom, Inc.*, No. 08-02047, 2009 WL 347285, at *8 (S.D. Cal. Feb. 6, 2009) (citing 18 U.S.C. § 1030(c)(4)(A)(i)), *vacated on other grounds*, 718 F. Supp. 2d 1232, 1240 (S.D. Cal. 2009); *see also Bose v. Interclick, Inc.*, No. 10-9183, 2011 WL 4343517, at *6 (S.D.N.Y. Aug. 17, 2011); *DoubleClick*, 154 F.

Supp. 2d at 524-26; *LaCourt*, 2011 WL 1661532, at *6 n.4. Even courts that have mistakenly assumed aggregation by private plaintiffs is permissible have still required a showing of cognizable loss from a "single act" by the defendant. *See In re iPhone Application Litig.*, No. 11-2250, 2011 WL 4403963, at *11 (N.D. Cal. Sept. 20, 2011) ("*iPhone I*"). Plaintiffs here allege neither a cognizable loss nor a "single act" causing loss. *Supra* pp. 1-4. Instead, they allege that Google placed cookies on Safari and IE browsers in distinct ways (*see* CAC ¶¶ 84-94, 171-190), at different times, and in connection with Plaintiffs' visits to different websites.

2. Google Did Not Engage in Any "Hacking"

The CFAA is also inapplicable because Plaintiffs do not allege any "criminal" computer "hacking," but rather that Google interacted with their browser software as it was designed to operate. Mot. at 22. Plaintiffs' only response is that Google "hacked" their computers by "tricking" their browsers. Opp. at 23-24. But Google did not override a protection or exploit a loophole. According to Plaintiffs' own allegations, Google merely utilized a function intentionally designed into the browsers. CAC ¶¶ 76, 78, 180-84; RJN Ex. 3; Mot. at 6-9. It is implausible to suggest that software could be "tricked" when used as it was designed to function. Plaintiffs' inability to cite any authority holding that the CFAA prohibits interacting with the known default features of software only further confirms that their CFAA claim must fail, particularly when considered in conjunction with the rule of lenity. *See* Mot. at 25 & n.13.

3. Plaintiffs Have Not Shown a Transmission Offense or an Unauthorized-Access Offense

The CFAA claim also fails because Plaintiffs do not allege facts showing that: (1) Google intended to cause damage (required for a transmission violation); (2) Google intentionally accessed Plaintiffs' browsers without authorization and resulting damage *and* loss (required for an unauthorized-access violation); or (3) Google intentionally exceeded authorized access to their browsers and thereby obtained "information" (required for an exceeding-authorization violation). Plaintiffs do not even attempt to argue that they have alleged the required "intent to cause damage," "resulting damage *and* loss" or "obtained information" ele-

ments. *See* Opp. at 26-27. Their failure to meet these elements requires dismissal of the claim. Plaintiffs' sole argument in opposition—that Google attempted to "trick" their browsers (*id.*)—is refuted by their own allegations that Google used Plaintiffs' browsers as they were designed. In any event, pleading an "attempt to trick" does not satisfy any element of a CFAA claim.[8]

D. Plaintiffs Cannot State a California Computer Crime Law Claim

Plaintiffs' California Computer Crime Law ("CCL") claim fails for essentially the same reasons as Plaintiffs' CFAA claim: they allege no damage, no cognizable loss, and no facts showing Google acted knowingly and without permission to cause damage to their computers or to take their information. Mot. at 26-29. In response, Plaintiffs again rely on conclusory allegations about the purported diminution in value of their PII to show loss, but they do not identify any damage or address their failure to show that Google acted "knowingly" and "without permission." Opp. at 31-32. Consequently, this claim falls with their CFAA claim.

Plaintiffs do not even respond to the defects Google identified in four of the five CCL violations they allege, ignoring all but subsection 502(c)(8). *See* Mot. at 27-29; Opp. at 31. With respect to subsection 502(c)(8), Plaintiffs simply declare that Google's method of placing cookies on Safari browsers was a "computer contaminant." But the phrase "computer contaminant" contemplates malicious code that usurps or interferes with a computer's normal operation. *See* Cal. Pen. Code § 502(b)(10). Cookies are not malicious computer contaminants, and Plaintiffs do not allege any such usurpation or interference. *See* CAC ¶¶ 38-39.

E. Plaintiffs Cannot State a California Privacy Claim

Plaintiffs do not dispute that their state law "invasion of privacy" and "intrusion upon seclusion" claims are duplicative or that they must demonstrate a legally-protected privacy interest

[8] Plaintiffs also refer to a settlement between Google and the FTC to suggest Google acted with ill intent. *See* Opp. at 2, 13, 27. The FTC allegations were not premised on any "scheme" to "trick" browsers into accepting cookies and certainly do not reflect any nefarious plan at Google. Rather, the FTC contended that Google made a statement to certain users that it would not use cookies to serve targeted advertisements, but then did so. *United States v. Google Inc.*, No. 12-4177, D.I. 1 ¶ 12 (N.D. Cal. Aug. 8, 2012). Even for that very different claim, the FTC did not allege that Google intended to mislead anyone, or that anyone was, in fact, misled.

to state these claims. *See* Opp. at 27. The only "legally protected right" Plaintiffs claim is "to be free of Google's 'information gathering' and to conduct personal activity (web browsing) 'without observation' by Google." *Id.* But Plaintiffs cannot claim a right of privacy in the BGI they *voluntarily sent* to Google (and to countless sites they visited). *See* CAC ¶¶ 30-33, 41-46; *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) ("Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit"); *Hill v. Nat'l Coll. Athl. Ass'n*, 865 P.2d 633, 648 (Cal. 1994); *TBG Ins. Servs. Corp. v. Superior Court*, 117 Cal. Rptr. 2d 155, 164 (Cal. Ct. App. 2002). Nor can Plaintiffs demonstrate any protected privacy interest in preventing Google from "associating" multiple instances of BGI voluntarily sent by Plaintiffs' browsers.[9] *See, e.g.*, *London v. New Albertson's, Inc.*, No. 08-1173, 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) (no protected privacy interest in preventing pharmacy from correlating consumers' anonymized drug prescription information); *Google Privacy Policy*, 2012 WL 6738343, at *5 (plaintiffs could not "identif[y] a concrete harm from the alleged combination of their personal information across Google's products").

Moreover, the case law makes clear that merely associating multiple communications of BGI from the same browser is not a "serious invasion" of privacy. Mot. at 31 (citing cases); *see also Yunker*, 2013 WL 1282980, at *14-15 (distribution of personal information to advertising libraries for marketing purposes was not "an egregious breach of social norms" nor "offensive or objectionable to a reasonable person or highly offensive"). Plaintiffs do not even try to distinguish the cases Google cites on this point, and they provide no contrary authority. Because Plaintiffs cannot meet these required elements of their state law claims, the claims cannot stand.

[9] Plaintiffs also argue that they have a reasonable expectation of privacy in their browsing activity because their "browsers' default settings prohibited Google's tracking cookies." Opp. at 27-28. But Plaintiffs again ignore their own allegations that (i) their browsers send BGI to Google upon visiting a website with a Google ad *whether or not a cookie is present*, and (ii) their browsers did not "prohibit" Google's cookies from being placed on them—by default their browsers were designed to permit third party cookies to be placed in a number of circumstances. *See* CAC ¶¶ 30-33, 41-46, 78, 84-96, 180-84; Mot. at 6-9; RJN Ex. 3.

F. Plaintiffs Cannot State a California CLRA Claim

Plaintiffs' arguments in support of their California Consumer Legal Remedies Act ("CLRA") claim cannot salvage it. *See* Mot. at 31-33. *First*, while Plaintiffs acknowledge that the CLRA only applies in connection with a transaction for the sale or lease of consumer goods or services (Opp. at 34), the CAC contains no allegations that Plaintiffs purchased anything from Google's DoubleClick advertising business. Plaintiffs instead point to their *use* of websites that participate in Google's advertising network, arguing that "[t]he consideration for using the Google services is the payment of personal information to Google." *Id.* That does not qualify as a "transaction" under the CLRA because Google provided the "services" free to Plaintiffs. *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. 11-2258, 2012 WL 4849054, at *20-21 (S.D. Cal. Oct. 11, 2012); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 717 (N.D. Cal. 2011); *Wofford v. Apple Inc.*, No. 11-34, 2011 WL 5445054, at *2 (S.D. Cal. Nov. 9, 2011). Plaintiffs' contention that their personal information constitutes a form of "payment" to Google "is unsupported by law." *Facebook*, 791 F. Supp. 2d at 717; *see also Yunker*, 2013 WL 1282980, at *12 (dismissing CLRA claim where plaintiff alleged "he purchased the defendant's services with his PII" and not with money).

Second, the CLRA does not cover software activity. Mot. at 31-32. Plaintiffs try to avoid this fatal limitation by arguing that Google "sells a service, not software," and by claiming that the cases Google cites supposedly "deal exclusively with software purchases." Opp. at 33. Not so. Plaintiffs ignore the *Sony Gaming* case, which recently held that an online video gaming network "and other online services" are software activity not covered by the CLRA. *Sony Gaming*, 2012 WL 4849054, at *20-21 (dismissing CLRA claim). And Plaintiffs cannot distinguish the software services in *iPhone I*, 2011 WL 4403963, and *Ferrington v. McAfee, Inc.*, No. 10-1455, 2010 WL 3910169 (N.D. Cal. Oct. 5, 2010), from the software services here.

Third, Plaintiffs assert that "Google's actions harmed the value of their personal information" (Opp. at 34), but identify no facts showing how Google's alleged conduct caused a "tangible increased cost or burden" to them. Mot. at 32 (quoting *Meyer v. Sprint Spectrum L.P.*,

200 P.3d 295, 299 (Cal. 2009)). And Plaintiffs' citation to *Doe 1* is inapposite, since it involved (1) disclosure of highly sensitive personal information, including social security and credit card numbers, and (2) plaintiff's payment to AOL to keep information secure. *See Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1111 (N.D. Cal. 2010). No such facts are or could be alleged here.

G. Plaintiffs Cannot State a California Unfair Competition Claim

1. Plaintiffs Fail to Show They Have Standing Under the UCL

Plaintiffs admit that to have standing under California's Unfair Competition Law ("UCL") they must plead an "economic injury." Opp. at 29; *see Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 810-11 (N.D. Cal. 2011) (distinguishing economic injury under UCL from injury required for Article III standing). Plaintiffs further concede that their only alleged injury is a claimed diminution in the value of their "PII." Opp. at 29. This confirms that they lack UCL standing because "the loss of privacy or personal information does not meet the standing requirements of the UCL." Mot. at 34; *see also In re Google Android Consumer Privacy Litig.*, No. 11-2264, 2013 WL 1283236, at *8 (N.D. Cal. Mar. 26, 2013).

Plaintiffs fail to cite any case in which alleged diminution in value of PII was sufficient to establish UCL standing. Their reliance on *Fraley* is misplaced. The *Fraley* court rejected the argument that the alleged diminution in value of PII could confer UCL standing. *Fraley*, 830 F. Supp. 2d at 810-12 (economic injury found only in failure to receive statutory compensation for use of plaintiffs' names and likeness). Even if diminution in value of PII could confer UCL standing, Plaintiffs' claim to have alleged a "dollar value of their PII" (*see* Opp. at 30) fails, not only because they have made no such allegation (the CAC alleges potential values only of other types of PII not at issue here (*see supra* pp. 3-4)), but also because they fail to allege facts showing any actual diminution of *their own* PII. *See Yunker*, 2013 WL 1282980, at *4, *11.

2. Plaintiffs Fail to Show Causation

Plaintiffs cannot demonstrate the required causation between Google's alleged placement of cookies and the alleged diminution in value of Plaintiffs' PII. *See* Mot. at 34-35. As shown above, the alleged placement of cookies did not cause Google to receive any BGI from Plaintiffs.

Supra pp. 1-3. Plaintiffs allege no facts showing that the placement of cookies caused them to lose any specific opportunity to sell their information or resulted in its sale at a lesser value.

3. Plaintiffs Fail to Show that Any Prong of the UCL Applies

Plaintiffs acknowledge that even if they could allege an economic injury here, they would still need to allege conduct that was "unlawful," "fraudulent," or "unfair." *See* Opp. at 28-29. They fail to make this showing. Plaintiffs' claim under the "unlawful" prong is admittedly dependent upon their other claims and will fall with those claims. *See id*. at 28. Plaintiffs' argument under the "fraudulent" prong fails because it is based on an alleged misrepresentation about the Safari browser posted to an obscure page on Google's website that no Plaintiff alleges ever having viewed or relied upon. *See* CAC ¶¶ 79, 248-249; *see also In re Facebook PPC Advert. Litig.*, 709 F. Supp. 2d 762, 771 (N.D. Cal. 2010). Finally, Plaintiffs' argument under the "unfair" prong fails because, while they admit that an unfair practice is one where the "harm to themselves . . . outweighs the utility of [Google's] conduct" (Opp. at 28-29), they do not allege facts showing they were harmed or that any harm outweighed the utility of Google's placement of the DoubleClick ID Cookie. Nor could they make that showing where Google obtained no additional information from Plaintiffs by using the cookie and where its use of the cookie admittedly provided Plaintiffs with more "targeted, relevant and engaging" ad content. *See* CAC ¶ 43.

IV. CONCLUSION

For the foregoing reasons and the reasons explained in Google's opening brief, Google respectfully requests that the Consolidated Amended Complaint be dismissed.

Respectfully submitted,

Dated: April 26, 2013

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ *Michael H. Rubin*
Michael H. Rubin

Attorneys for Defendant
GOOGLE INC.